EIDAuthenticate 活用マニュアル

Pentio USB Token 3300A 付属パッケージ

Windows 8.1 / Windows 7
Startup Guide

2014/7/3

pentio

ペンティオ、Pentio およびそれらを含むロゴは日本および他の国におけるペンティオ株式会社の商標または登録商標です。

ジェムアルト、Gemalto およびそれらを含むロゴは日本および他の国におけるジェムアルト株式会社の商標または登録商標です。

Microsoft および Windows、Windows Vista、Windows Server は米国 Microsoft Corporation の米国、日本およびその他の国における登録商標です。

その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。

Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

本書の著作権はペンティオ株式会社に帰属します。著作権法の認める範囲を除き、本書を無断で複製、複写、改変、デジタルデータに変換すること、および営利非営利を問わず再配布、譲渡することを禁じます。

目次

目次 3

1. はじめに 4

1.1. はじめに 4
1.2. 対応 OS 4
1.3. 設定手順（概要） 5
1.4. 用語について 6

2. インストール 7

2.1. 管理者アカウントでログオンする 7
2.2. スマートカードをセットアップする 7
2.3. EIDAuthenticate をインストールする 8

3. スマートカードログオンを設定する 11

3.1. 証明書が入ったスマートカードを用意する 11
3.1.1. EIDAuthenticate を起動する 12
3.1.2. 認証局と証明書を作成する 14
3.2. アカウントに証明書を紐付ける 17
3.3. 高度な使い方 20

4. スマートカードでログオンする 21

5. セキュリティを強化する 22

5.1. Windows ログオンのパスワードを変更する 22
5.2. スマートカード取り外し時の挙動を設定する 22
5.3. スマートカードを必須にする 24

6. IT 担当者の方へ 25

6.1. 他のアカウントに証明書を発行・紐付けるには 25
6.2. 複数の PC を管理する 26
6.2.1. 複数の PC に管理者カード（複数の証明書）でログオンするには 26
6.2.2. 複数の PC に管理者カード（一つの証明書）でログオンするには 27

7. Q&A 28

1. はじめに

1.1. はじめに

このたびは弊社製品をお買い上げいただき、ありがとうございました。

本書では Pentio USB Token 3300 シリーズおよび Pentio IC Card 3300 シリーズを用いて MySmartLogon 社製 EIDAuthenticate をご利用いただく方法について解説しています。

1.2. 対応 OS

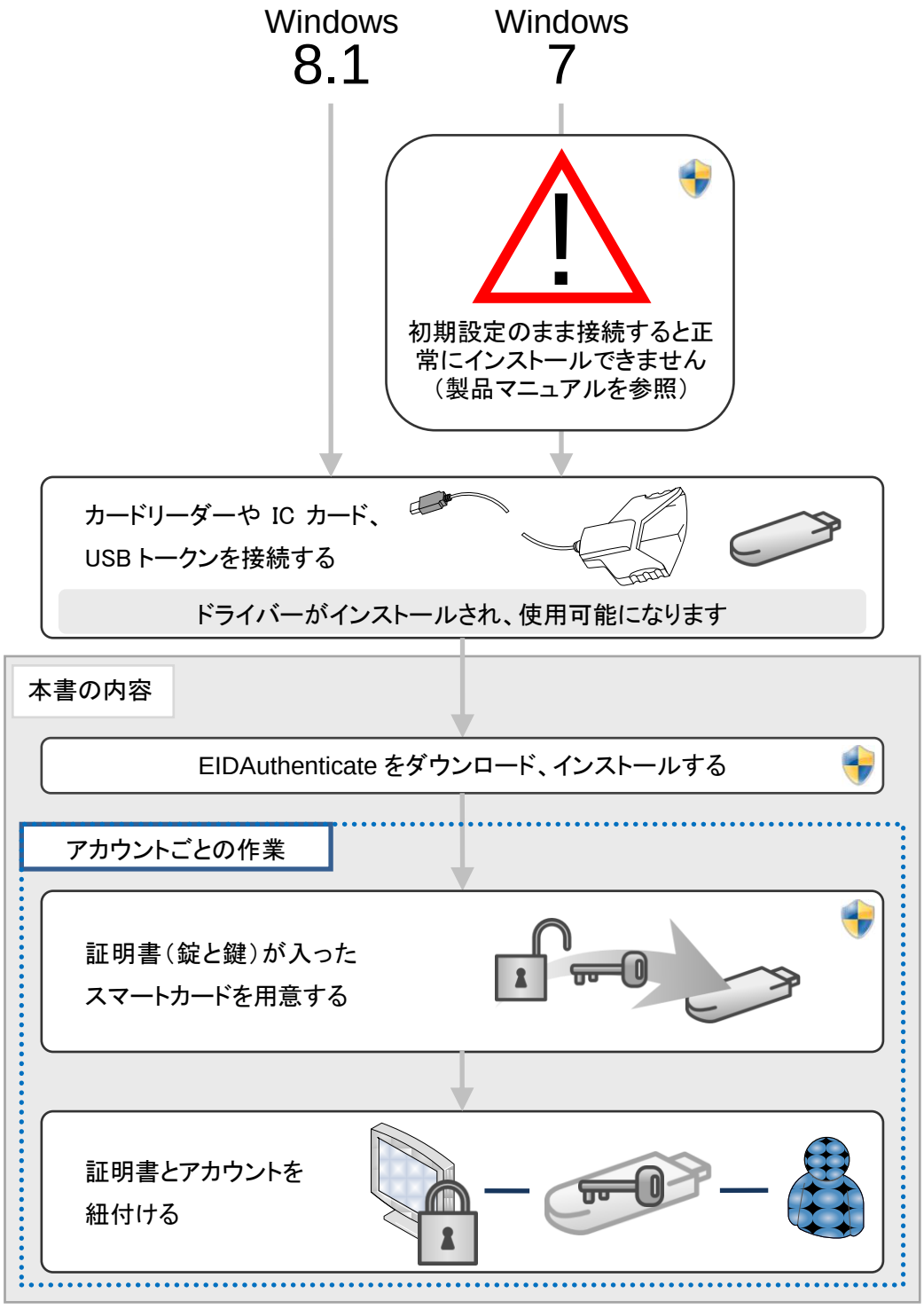
Pentio USB Token 3300 シリーズおよび Pentio IC Card 3300 シリーズは Windows 7 とWindows 8.1 / 8 のすべてのエディションに対応しています。詳細は各製品のカタログまたはマニュアルをご覧ください。

EIDAuthenticate は無償版と有償版があり、対応 OS が異なります。あらかじめご確認ください。

	Community Edition	Enterprise Edition
Windows 8.1 / 8	（無印）エディションのみ	すべてのエディション
Windows 7	Home Premium	すべてのエディション

本パッケージの EIDAuthenticate Enterprise Edition は Windows XP、Windows Vista に対応しておりません。旧 OS 対応版をご希望の方は弊社にお問い合せください。

1.3. 設定手順（概要）



このアイコンがある操作では管理者特権が必要です

1.4. 用語について

本書で扱う主要な用語について解説します。Microsoft の表記と一部異なることがありますのでご留意ください。

スマートカード

> USB トークンと IC カードをまとめてスマートカードと呼びます。本書で「スマートカードを挿入する」という表記は「USB トークンを USB コネクタに接続する」か「IC カードを IC カードリーダーに挿入する」ことを意味します。

スマートカードログオン

> Windows へのログオンに際して、「ID とパスワード」ではなく「スマートカードと PIN」を用いる認証をスマートカードログオンと呼びます。EIDAuthenticate はスマートカードログオンを実現するソフトウェアです。

管理者

> 管理者特権をもつアカウントを管理者と呼びます。

一般ユーザー

> 管理者特権をもたないアカウントを一般ユーザーと呼びます。

IT 担当者

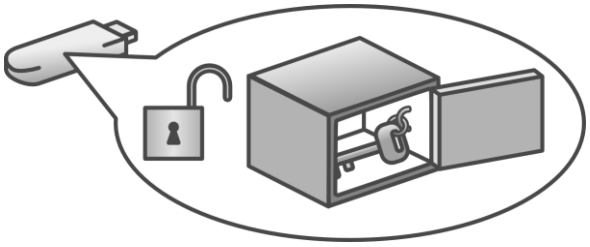
> 複数の PC を管理する立場にある人を IT 担当者と呼びます。

PIN

> スマートカードに設定される暗証番号です。変更方法はスマートカードの取扱説明書をご覧ください。

証明書

> スマートカードログオンは、いわば Windows を施錠することになります。その施錠で使う「錠」と「錠の情報」、対応する「鍵」をまとめたものを証明書と呼びます。スマートカードに書き込まれた「鍵」は PIN を入力することで利用できます。ただし、「鍵」自体をスマートカードから取り出すことはできません。



2. インストール

本章では EIDAuthenticate のインストール手順を解説します。

2.1. 管理者アカウントでログオンする

EIDAuthenticate のインストールには管理者特権が必要です。

2.2. スマートカードをセットアップする

スマートカードのインストールは各製品のマニュアルをご覧ください。

Pentio 製品は、自動インストールが有効であれば接続するだけでインストールされます。

自動インストールが有効になっているかを調べるには、スタートメニューまたは検索チャームにて「デバイスのインストール設定の変更」を検索し、検索結果を実行してください。

Windows 7 の場合は自動インストールが無効になっていることがあります。Pentio USB Token 3300 シリーズまたは Pentio IC Card 3300 シリーズの製品マニュアルをご覧になり、セットアップしてください。

2.3. EIDAuthenticate をインストールする

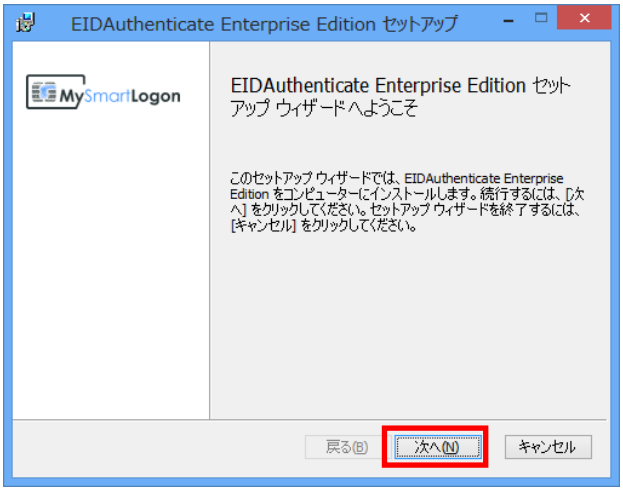
以下、Windows 8.1 の画面で解説します。

[1] CD-ROM を挿入し、EIDAuthenticate フォルダを開きます。

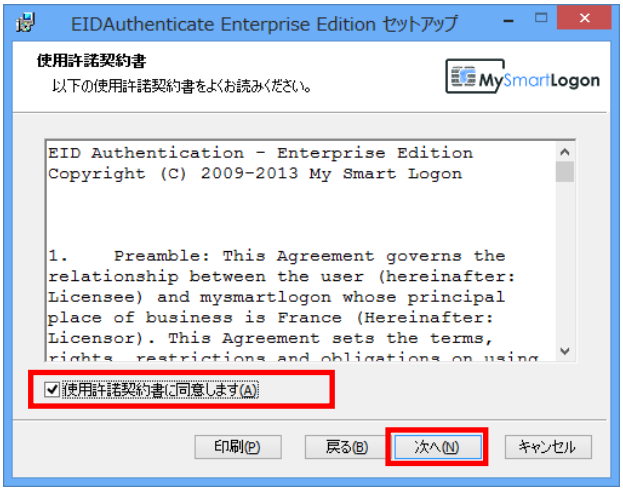
[2] セットアッププログラムを起動します。お使いの OS に合わせて選択してください。

32bit OS	EIDAuthenticateSetup_Enterprise-Edition_1.0.1.0_x86.msi
64bit OS	EIDAuthenticateSetup_Enterprise-Edition_1.0.1.0_x64.msi

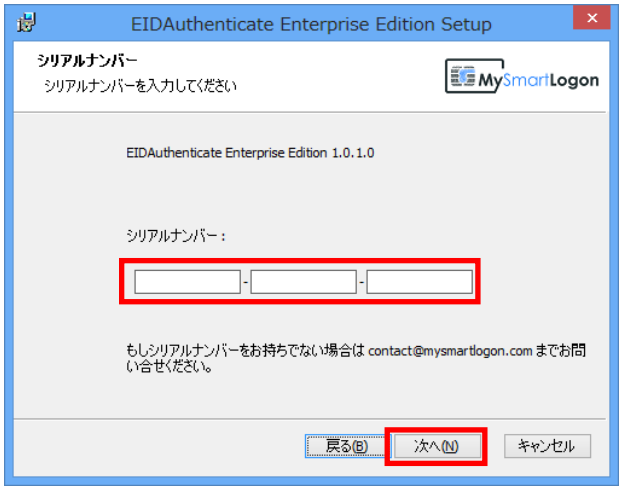
[3] ウィザードが起動します。「次へ」をクリックします。



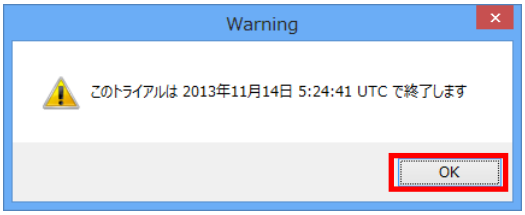
[4] 利用規約に同意し、「次へ」をクリックします。


EIDAuthenticate Enterprise Edition セットアップ
使用許諾契約書
以下の使用許諾契約書をよくお読みください。
MySmartLogon
EID Authentication - Enterprise Edition
Copyright (C) 2009-2013 My Smart Logon
1. Preamble: This Agreement governs the relationship between the user (hereinafter: Licensee) and mysmartlogon whose principal place of business is France (Hereinafter: Licensor). This Agreement sets the terms,
使用許諾契約書に同意します(A)
印刷(P)
戻る(B)
次へ(N)
キャンセル

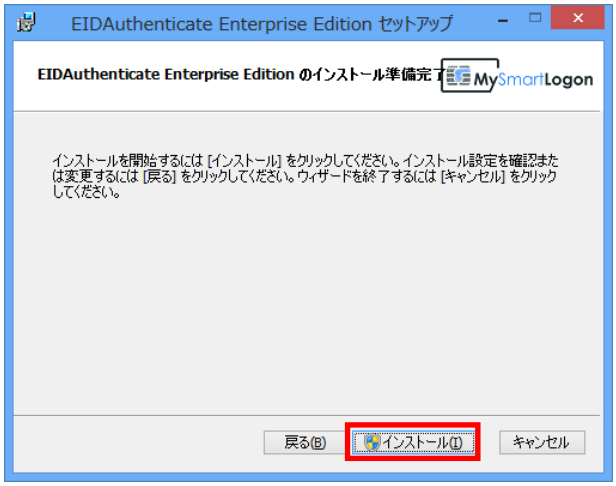
[5] パッケージに同梱されているシリアルナンバーを入力し、「次へ」をクリックします。



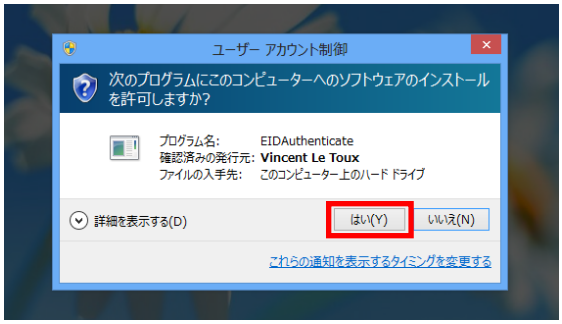
[6] 有効期限が設定されている場合、次のメッセージが表示されます。



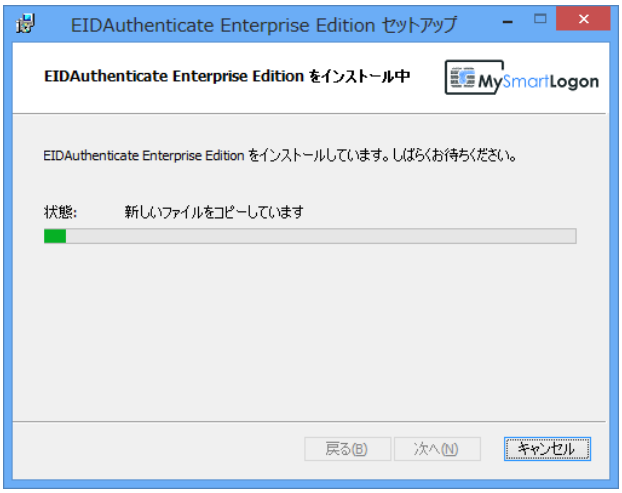
[7] 「インストール」をクリックします。



[8] 実行に際して警告が表示されますので、「はい」をクリックします。



[9] インストールが行われます。



[10] インストールが完了します。「完了」をクリックします。ここで「設定ウィザードを起動する」にチェックを付けておくと、「完了」クリック後に EIDAuthenticate が起動します。

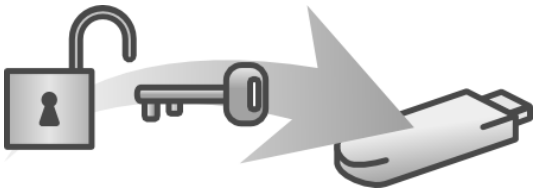
以上でインストールは完了です。

3. スマートカードログオンを設定する

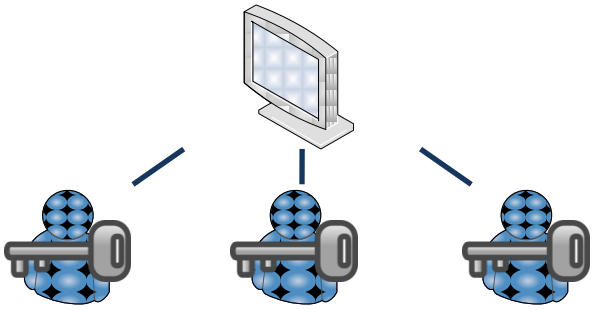
各アカウントに対して、スマートカードログオンを設定します。

3.1. 証明書が入ったスマートカードを用意する

EIDAuthenticate は必要な証明書（錠と鍵）を発行してスマートカードに書き込む機能をもっています。はじめてスマートカードをご利用になる場合でも簡単に作成できます。



一つのコンピューターでは、ユーザーアカウントと証明書（錠と鍵）は一対一で対応します。紐付けるアカウントごとに証明書を用意する必要があります。



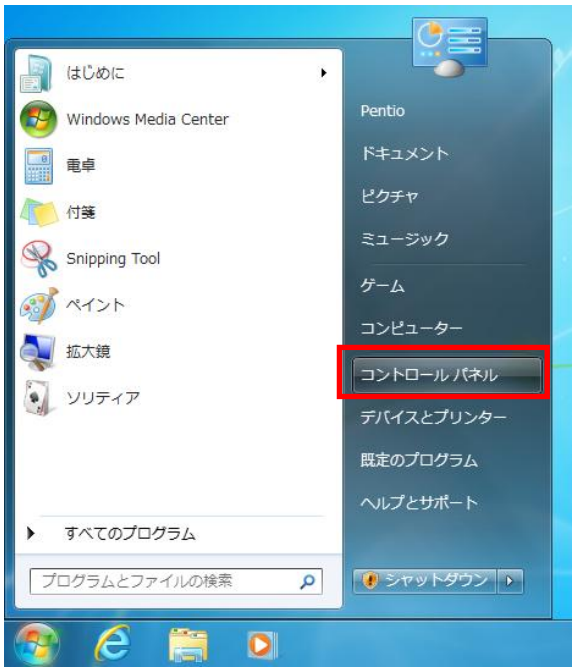
なお、すでに「当該コンピューターのどのアカウントにも紐付いていない証明書」が入ったスマートカードをお持ちの場合は、以下の手順をスキップし次節にお進みください。

3.1.1. EIDAuthenticate を起動する

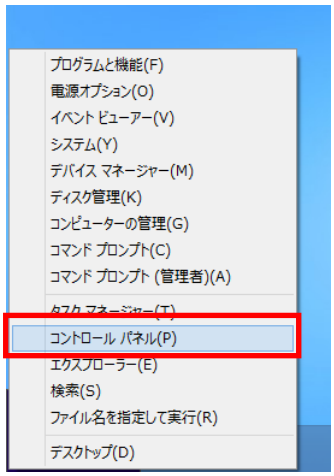
前章で「設定ウィザードを起動する」にチェックをつけていた場合、この項は飛ばしてください。

EIDAuthenticate はコントロールパネルから起動します。

[1] コントロール パネルを開きます。Windows 7 ではスタート メニューの「コントロール パネル」をクリックします。Windows 8.1 / 8 では画面左下で右クリックして表示されるメニューで「コントロール パネル」をクリックします。



Windows 7
スタートメニューをクリックします



Windows 8.1
画面左下を右クリックします

[2] 「システムとセキュリティ」をクリックします。

[3] 「スマートカードログオン」をクリックします。

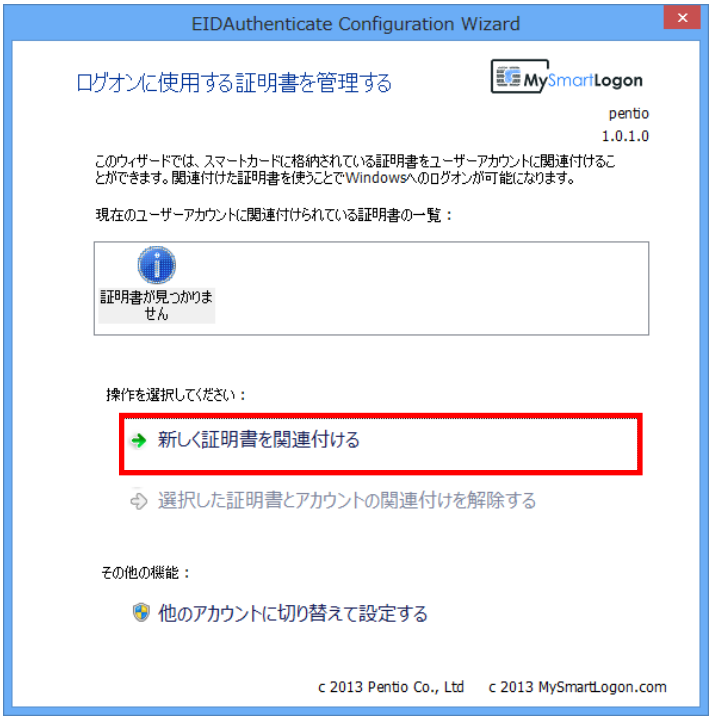
[4] EIDAuthenticate が起動します。

この画面では、ユーザーアカウント（右上に表示されています）と証明書の紐付け状況（上図は何も紐付けられていない状態）を確認できます。

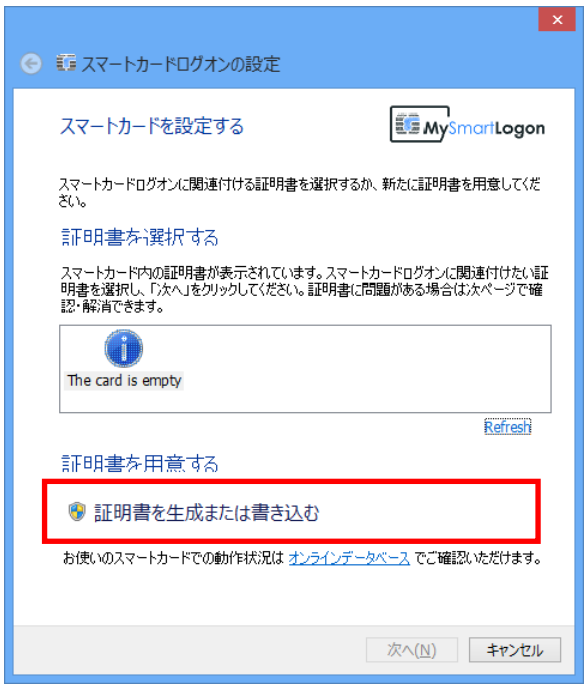
管理者として他のアカウントに対して操作するには **6.1. 他のアカウントに証明書を発行・紐付けるには** をご覧ください。

3.1.2. 認証局と証明書を作成する

[1] EIDAuthenticate を起動し、「新しく証明書を関連付ける」をクリックします。

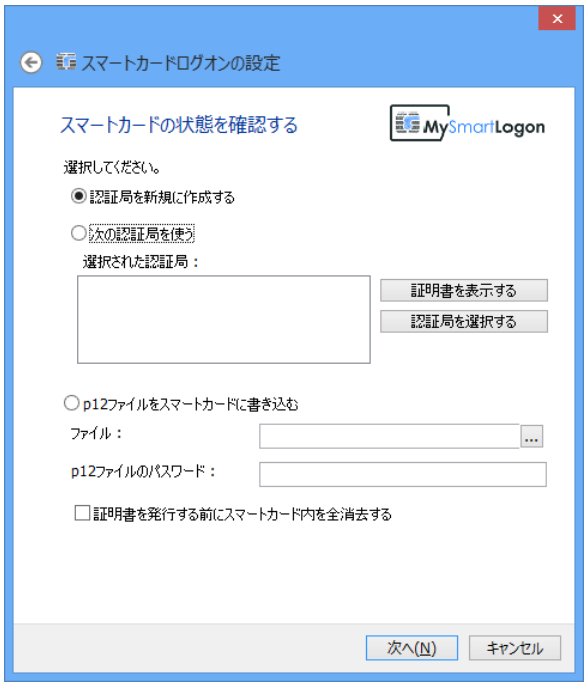


[2] 「証明書を選択する」か「証明書を用意する」を選択する画面になります。この時点ではスマートカードに証明書がありませんので、「証明書を生成または書き込む」をクリックします。警告が表示されるので続行します。



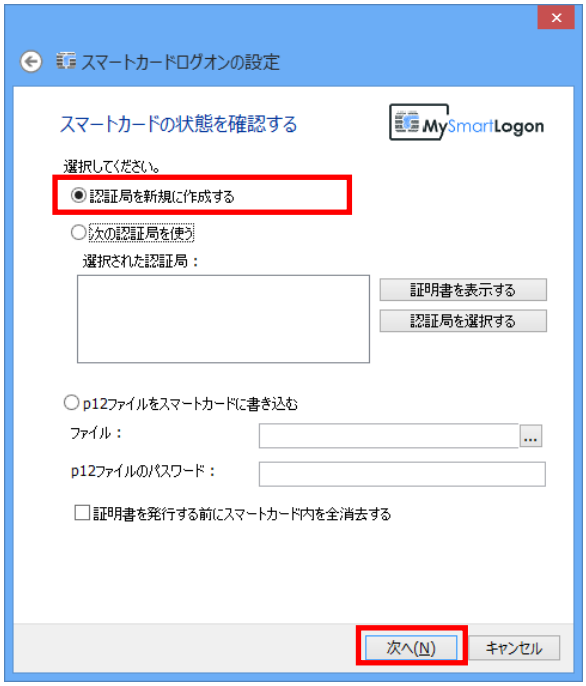
「スマートカードを挿入してください」などのメッセージが表示された場合は USB トークン、IC カードの取扱説明書をご覧になり、インストール状況を確認してください

[3] 証明書を作成するツールが起動します。

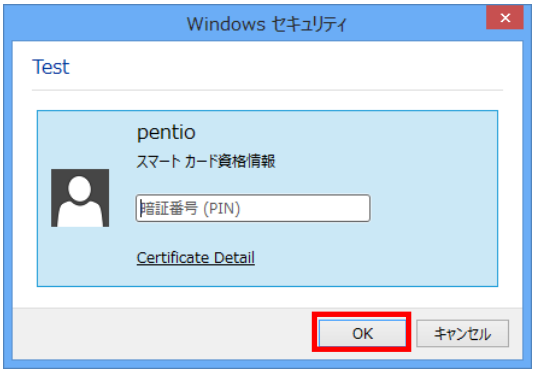


- お使いのコンピューターで初めてこの機能を使う場合、一番上の「認証局を新規に作成する」を選択します。この機能を選択すると、認証局の作成、証明書の発行、スマートカードへの書き込みが行われます。
- 二つ目以降のアカウントに対して証明書を発行する場合は、すでに認証局が作られた状態（中央の「選択された認証局」に認証局が表示されている状態）ですので、「次の認証局を使う」を選択します。この機能を選択すると、証明書の発行とスマートカードへの書き込みが行われます。

[4] 「次へ」をクリックします。



[5] スマートカードの PIN を入力し、「OK」をクリックします。



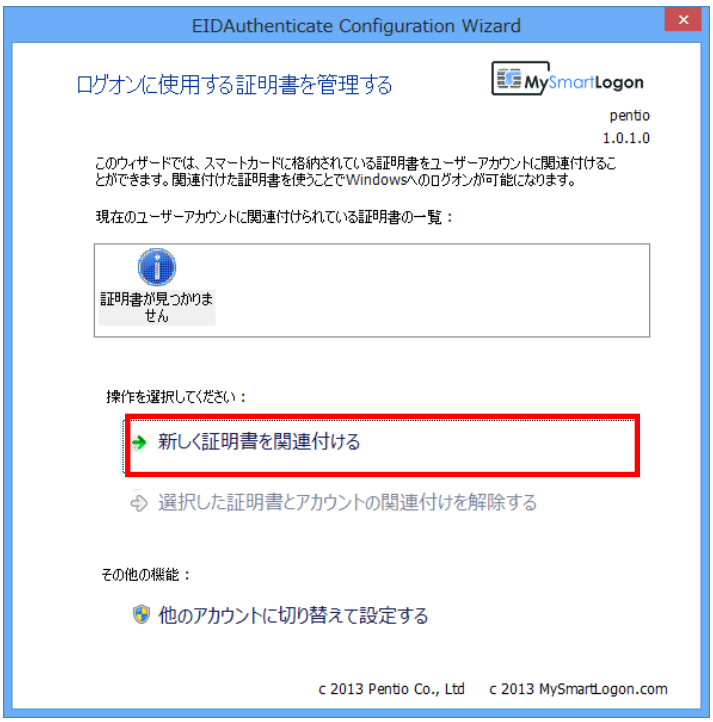
[6] 証明書の書き込みが行われます。画面が固まったようになりますが、数秒から数十秒そのままでお待ちください。作成される証明書の名前はアカウント名と同一です。

[7] 書き込みが完了すると、証明書の選択画面が起動します。次節にお進みください。

3.2. アカウントに証明書を紐付ける

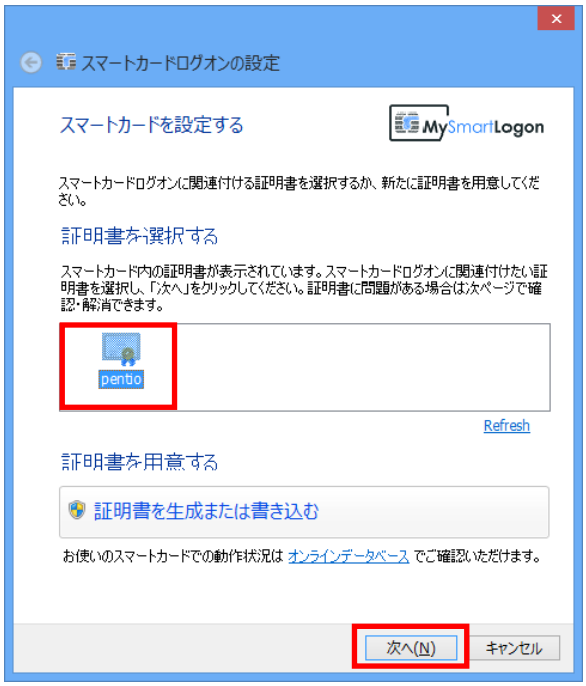
証明書が書き込まれたスマートカードを用意したら、その証明書とログオンアカウントを紐付けます）。

[1] EIDAuthenticate を起動し、「新しく証明書を関連付ける」をクリックします。（前節からの続きの場合、この画面は表示されません）



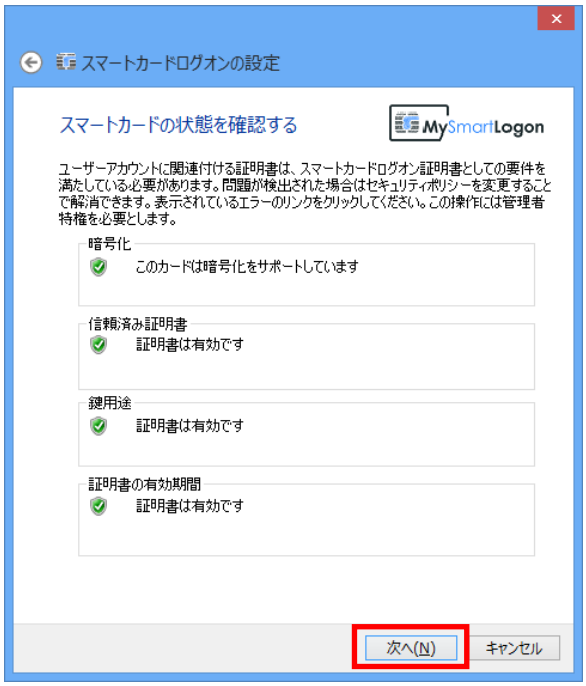
一つのユーザーアカウントに対して複数の証明書を紐付け、スペアキーを作成できます→ **3.3. 高度な使い方**（20 ページ）

[2] アカウントと紐付ける証明書を選択し、「次へ」をクリックします。

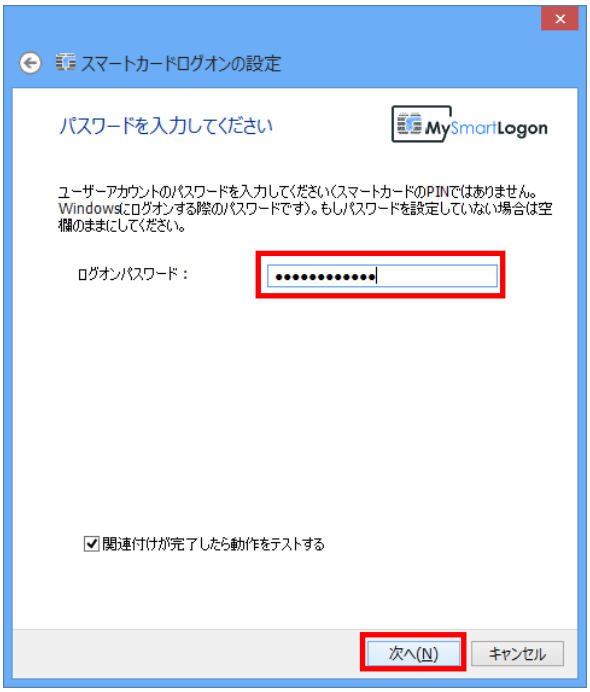


一つの証明書は一つのアカウントに紐付きます。すでに紐付けがなされた証明書は選択しないでください。

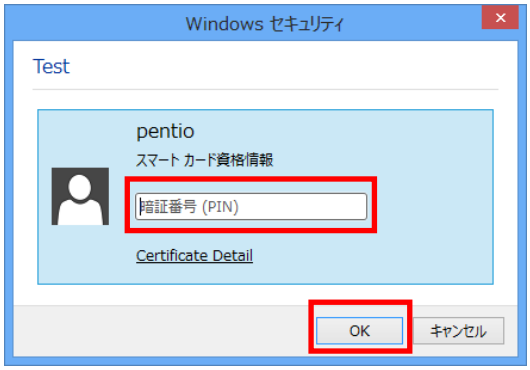
[3] 証明書の状態がチェックされます。「次へ」をクリックします。



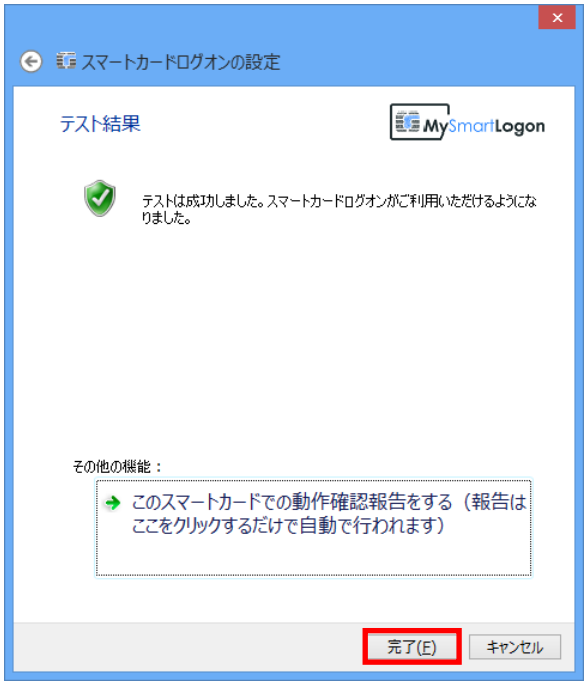
[4] ログオンパスワードの入力を求められますので、入力します（スマートカードの PIN ではなく、Windows にログオンする際に入力するパスワードです）。「次へ」をクリックします。



[5] 「関連付けが完了したら動作をテストする」にチェックを付けておくと、紐付けが成功したかテストが行われます。スマートカードの PIN を入力し、OK をクリックします。

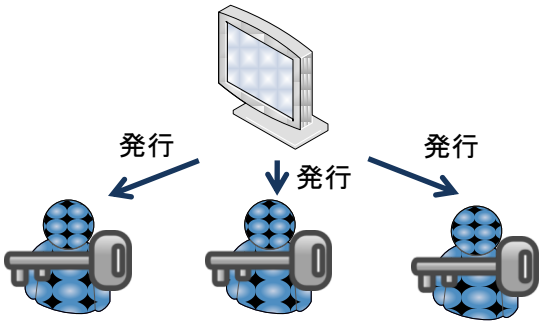


[6] 設定が完了した旨が表示されます。「完了」をクリックして終了します。



以上で、Windows ログオンでスマートカードをご利用いただけるようになりました。

他のアカウントでスマートカードログオンを使う場合は、本章の内容（アカウントの選択、証明書の発行と紐付け）を再度行なってください。



3.3. 高度な使い方

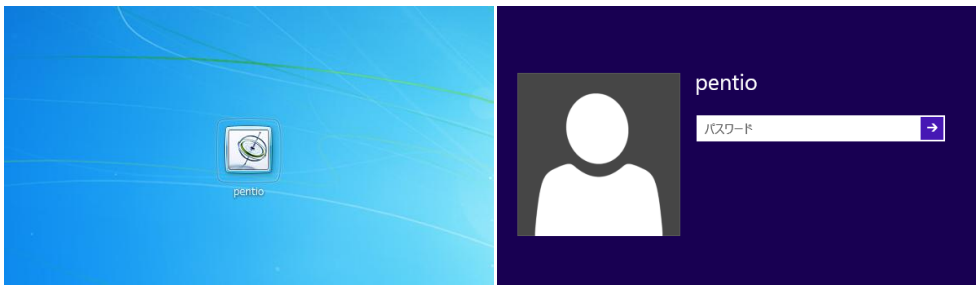
一つのアカウントに対して、複数の証明書を紐付けることも可能です。これを利用して、スペアキーを作ることができます。

新規のスマートカードを挿入し、**3.1.2. 認証局と証明書を作成する** からの手順を行って下さい。

4. スマートカードでログオンする

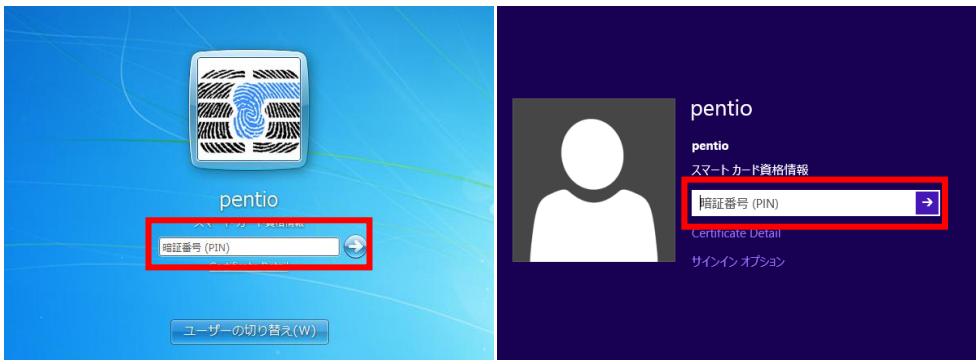
本章ではスマートカードログオンを設定したアカウントでログオンする方法を解説します。

[1] Windows を起動します。(ログオフ後やロック時も同様です。)



[2] スマートカードを挿入します。画面が切り替わるので、スマートカードの PIN を入力し、Enter キーを押すか「→」アイコンをクリックします。

> 画面が切り替わらない場合はユーザーの切り替え(W)ボタンを押してスマートカードログオン設定したアカウントに切り替えを行ってください。



[3] カードの証明書情報に基づきログオン処理が行われます。

以上でログオンは完了です。

なお、起動時にスマートカード(USB トークン、IC カード)を接続していると[1]の画面を経由せず[2]の画面が表示されることもありますが、正常です。

5. セキュリティを強化する

ここまでの設定により、スマートカードでもログオンできるようになりました。しかしこれだけではセキュリティ強度を高めたとは言えません。本章ではスマートカードログオンを使い、セキュリティ強度を高める方法を解説します。

5.1. Windows ログオンのパスワードを変更する

スマートカードログオンを設定するまでは「覚えられるパスワード」を設定していることがほとんどです。このパスワードが漏洩するとセキュリティ上の脅威になります。

[1] 通常時のログオンにはスマートカードを用いることとし、パスワードは「非常用」と位置づけます。

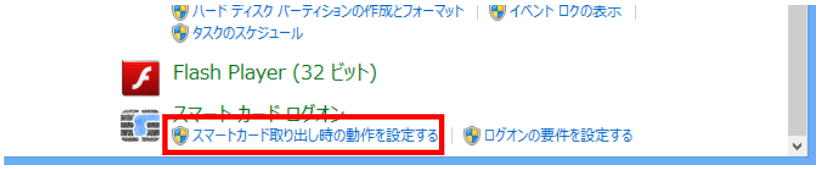
[2] パスワードをランダムで非常に長いものに設定します。このパスワードは紙に書き金庫に厳重に保管するなどして非常時のみ使用するものとします。

> パスワードやユーザー名を変更しても、設定したスマートカードは引き続き有効です

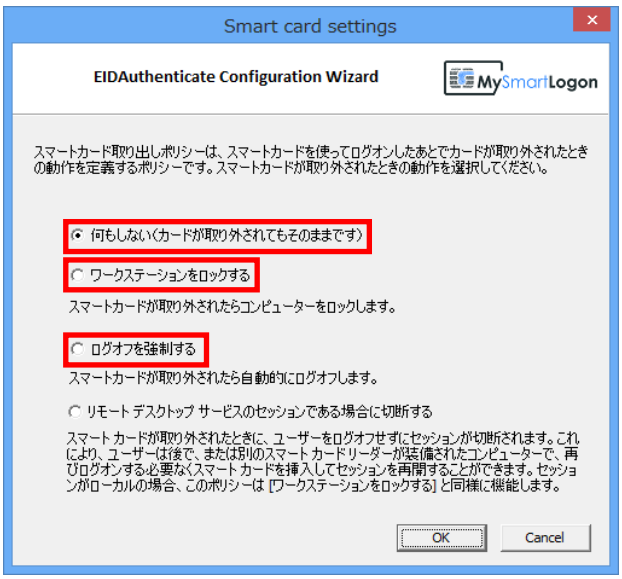
5.2. スマートカード取り外し時の挙動を設定する

スマートカードを抜き取ると、自動でロックをかけたりログオフしたりといった設定が可能です。

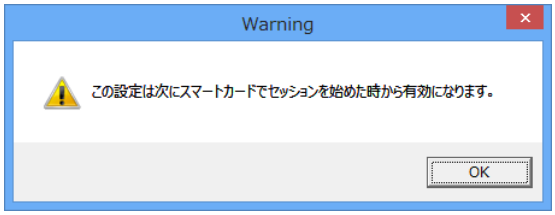
[1] コントロール パネルの「システムとセキュリティ」を開き、「スマートカード取り出し時の動作を設定する」をクリックします。



[2] 初期設定では「何もしない」になっています。「ワークステーションをロックする」でスマートカード取り外し時にコンピューターをロックする、「ログオフを強制する」でスマートカード取り外し時にログオフする設定になります。



[3] この設定は次にスマートカードでログオンしたときから有効になります。



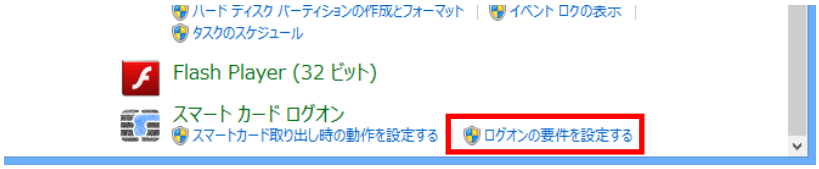
以上でスマートカード取り出し時の挙動の設定は完了です。

5.3. スマートカードを必須にする

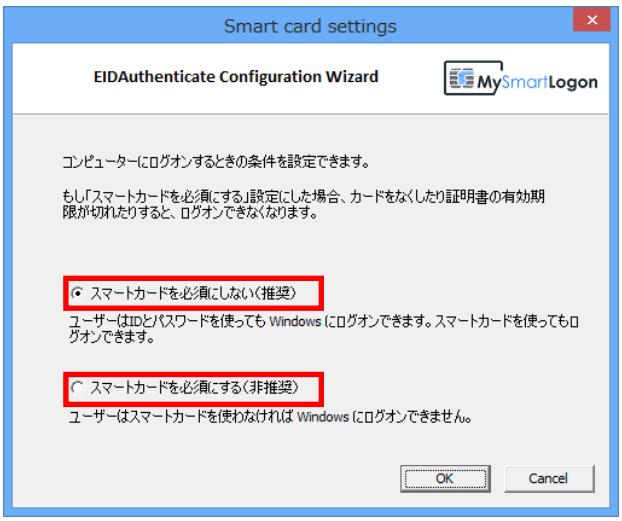
スマートカードで認証ができるようにしただけでは、アカウント名とパスワードを使った以前の方法でもログオンできます。本節ではログオンをスマートカードログオンに限定する方法について解説します。

以下の「スマートカードを必須にする」設定にした場合、非常に高いセキュリティを実現できますが、**スマートカードを紛失するとPCにログオンできなくなります**。スマートカードがなければいかなる方法でも解除できませんのでご注意ください（弊社にお問い合わせいただいても解除することはできません）

[1] コントロール パネルの「システムとセキュリティ」を開き、「ログオンの要件を設定する」をクリックします。



[2] 初期設定では「スマートカードを必須にしない（推奨）」になっています。「スマートカードを必須にする（非推奨）」を選択するとログオン時には必ずスマートカードが必要になります。（このオプションを選択する場合は、スペアとなるスマートカードを作成・設定しておくことを強く推奨します）



設定は次回ログオン時から有効になります。

6. IT 担当者の方へ

6.1. 他のアカウントに証明書を発行・紐付けるには

3.1.2. 認証局と証明書を作成する や **3.2. アカウントに証明書を紐付ける** ではログオン中のユーザーアカウントに対して証明書を発行したり紐付けたりを行いましたが、他のアカウントに対してもこれらの操作を実行できます。

下記画面で、「他のアカウントに切り替えて設定する」をクリックしてアカウントを検索・選択すると右上のアカウント名が変わります。以後の操作では発行と紐付けをそのアカウントに対して行うことができます。

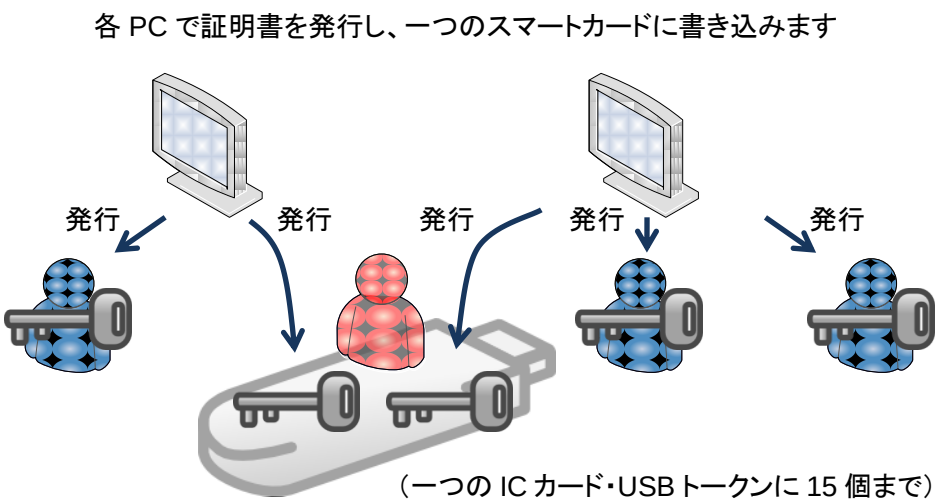
6.2. 複数の PC を管理する

複数台の PC を管理する立場の方向けに、一枚のスマートカードで複数台にログオンできる方法を解説します。

6.2.1. 複数の PC に管理者カード（複数の証明書）でログオンするには

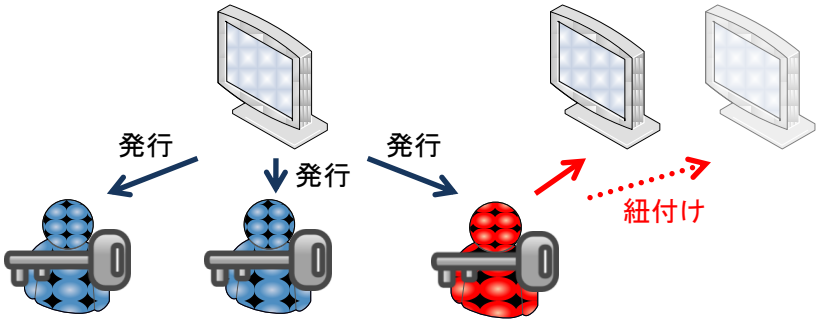
Pentio USB Token 3300 シリーズと Pentio IC Card 3300 シリーズは、最大で 15 個の証明書を格納できます。

操作方法は 1 個だけ入れる際の発行手順と同様です。各 PC で証明書の発行を行なってください。



6.2.2. 複数の PC に管理者カード（一つの証明書）でログオンするには

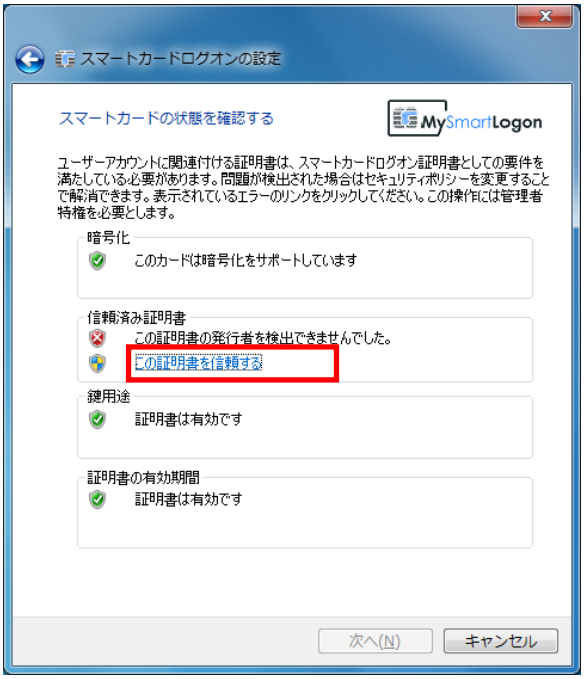
同じコンピューター内で一つの証明書を複数のアカウントに紐付けることはできませんが、異なるコンピューターであれば一つの証明書を使いまわすことが可能です。



[1] 一台目の PC でスマートカードログオンを設定します。

[2] 二台目の PC で **3.2. アカウントに証明書を紐付ける** を行います。

[3] 証明書を発行した PC ではないため、「この証明書の発行元を検出できませんでした」というエラーが表示されます。「この証明書を信頼する」をクリックし、「次へ」をクリックします。以降の操作は 1 台目の PC と同一です。



7. Q&A

Q. 使っている OS のエディションや 32bit/64bit がわからない

A. [Windows 7 の場合] スタートメニューの「システム」を右クリックし、「プロパティ」をクリックします。

A. [Windows 8.1 / 8 の場合] 画面左下を右クリックし、「システム」をクリックします。

Q. スマートカードログオンを設定したあとで、パスワードやアカウント名は変更しても大丈夫でしょうか？

A. 問題ありません。パスワードはより強固なものに変更することをお勧めします。

Q. スマートカード内に証明書はいくつ格納できますか？

A. Pentio USB Token 3300 シリーズおよび Pentio IC Card 3300 シリーズには最大 15 個の証明書を格納できます。

Q. 発行した証明書の有効期限は？

A. 10 年間です。この有効期限を過ぎるとスマートカードでログオンできなくなります。

Q. EIDAuthenticate 以外で発行した証明書は使えますか？

A. ご利用いただけます。ただし、関連付けには細心の注意を払ってください。特に証明書の有効期限は絶対にご確認ください。証明書によっては有効期限が 1 年程度に設定されているものもあり、それを過ぎるとログオンできなくなります。

Q. スマートカードを紛失するとログインできなくなるんでしょうか？

A. 通常の設定ですと、パスワードを入力することでもログインできます。一方、コントロールパネルの「ログオンの要件を設定する」で「スマートカードを必須にする」設定も可能です（推奨されません）。なお、一つのアカウントに複数の証明書を紐付けることもできますので、ログオンに使えるカードを複数枚作成しておくことは可能です。

お問い合せ

ペンティオ株式会社
PKI ソリューション事業部
Tel: 03-5919-0971
Mail: sales@pentio.com
Site: http://www.pentio.com